УДК 004.04
В.О. Заводянський
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ЗАХИСТ ІНФОРМАЦІЇ В ЕЛЕКТРОННОМУ ДОКУМЕНТООБІГУ

V.O. Zavodyanskiy

PROTECTION OF INFORMATION IN THE ELECTRONIC DOCUMENT SECURITY

Широке використання інформаційних технологій у всіх сферах життя суспільства робить досить актуальною проблему захисту інформації, інформаційних ресурсів, каналів передачі даних від злочинних дій зловмисників. У міру розвитку технологій електронних платежів та документообігу є велика небезпека втручання сторонніх осіб, з метою завдання шкоди підприємству, що призведе до відчутних збитків. Тому не випадково захист даних у комп'ютерних мережах стає однією із найгостріших проблем.

Використання систем електронного документообігу (СЕД) дозволяє досягти величезного економічного ефекту. Але, упроваджуючи СЕД не можна забувати про безпеку системи. Однією з найважливіших вимог до будь-якої СЕД є забезпечення безпеки електронного обміну документами.

Основними загрозами безпеки СЕД є:

- Загроза цілісності інформації;
- Загроза конфіденційності;
- Загроза роботі системи;
- Загроза доступності.

Особливе значення має регулювання (регламентування) документообігу, яке пов'язане з електронними документами.

Регламент документообігу являє собою сукупність правил інформаційної діяльності суб'єктів інформаційних відносин, визначених законодавством, нормативними актами або угодами. Регламент документообігу визначає ролі та права суб'єктів щодо створення, володіння, користування та розпорядження документами, порядок оформлення і фіксації інформації на носієві інформації.

Відповідно до статті 6 Закону України «Про електронні документи та електронний документообіг»[1] електронний підпис є обов'язковим реквізитом електронного документу (ЕД), який використовується для ідентифікації автора та/або підписувача ЕД іншими суб'єктами електронного документообігу.

Статтею 1 Закону України "Про електронний цифровий підпис"[2] визначено такі терміни:

- електронний підпис – дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних;
- електронний цифровий підпис (ЕЦП) – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа;

Захищеність ЕЦП від відтворення чи підробки базується на застосуванні у відповідних технологіях методів криптографії. Так, у разі застосування алгоритму для

формування та перевіряння електронного цифрового підпису з довжиною ключа у 264 біти тривалість часу, необхідного для його можливого "зламування" шляхом застосування найсучасніших методів криптоаналізу з допомогою комп'ютера із частотою процесора у 3 ГГЦ, експерти оцінюють величиною майже 1 тис. років.

Для забезпечення захисту інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах повинні обов'язково виконуватися наступні процедури:

– автентифікація – процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора;

– ідентифікація – процедура розпізнавання користувача в системі, як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою.

Для організації захисту інформації електронної системи документообігу додаткову увагу потрібно звернути на забезпечення доступності публічної ніформації та блокування несанкціонованого доступу. Основне проблемне місце при організації захисту СЕД – це не технічні засоби, а лояльність користувачів. Як тільки документ потрапляє до користувача, конфіденційність цього документа по відношенню до користувача вже порушена. Технічними заходами в принципі неможливо запобігти витоку документа через цього користувача. Він може знайти безліч способів скопіювати інформацію, від збереження його на зовнішній носій до банального фотографування. Протоколювання дій користувачів – важливий пункт захисту електронного документообігу. Його правильна реалізація в системі дозволить відстежувати всі неправомірні дії і знайти винуватця, а при оперативному втручанні навіть зупинити спробу неправомірних або завдаючих шкоди дій.

Підхід до захисту електронного документообігу має бути комплексним. Необхідно тверезо оцінювати можливі загрози та ризики СЕД і величину можливих втрат від загроз. Захист СЕД не зводиться лише до захисту документів і розмежування доступу до них. Важливими є питання захисту апаратних засобів системи, персональних комп'ютерів, принтерів та інших пристроїв; захисту мережевого середовища, в якому функціонує система, захист каналів передачі даних і мережевого устаткування, можливе виділення СЕД в особливий сегмент мережі. Комплекс організаційних заходів відіграє важливу роль на кожному рівні захисту. Погана організація може звести нанівець усі технічні заходи, як досконалі вони б не були. При виборі засобів захисту слід оцінити реальні втрати від розголошення або спотворення інформації і співставити з вартістю засобів охорони. Але в будь-якому випадку повинні бути впроваджені елементарні, найдешевші і від цього не менш ефективні засоби – вхід до системи документообігу повинен здійснюватися за системою паролів з розмежованим рівнем доступу. Фізичний доступ в приміщення, де встановлена система керування документообігом, повинен здійснюватися за правилами внутрішнього розпорядку і бути обмеженим для сторонніх осіб.

Література

1. Про електронні документи та електронний документообіг [Електронний ресурс] – Режим доступу: URL: http://zakon1.rada.gov.ua/laws/show/851-15 – Дата доступу: 06.11.2017 – Назва з екрану.

2. Про електронний цифровий підпис [Електронний ресурс] – Режим доступу: URL: http://zakon2.rada.gov.ua/laws/show/852-15 – Дата доступу: 06.11.2017 – Назва з екрану.